**Amendments to the Specification:**

The following amendments refer to page and line numbers of the specification as originally filed. No new matter has been added.

1. Please replace the paragraph on page 1, lines 25-27 with the following amended paragraph:

The invention relates to methods and ~~apparata~~ apparatus for the secure communication of data, and more specifically to methods and ~~apparata~~ apparatus for the delivery of encrypted data across publicly-accessible networks.

2. Please replace the paragraph on page 7, lines 21-22 with the following amended paragraph:

~~Figure 5 illustrates~~ Figures 5A-5C illustrate in flow diagram form the Key Exchange protocol by which keys are exchanged between sender and receiver.

3. Please replace the paragraph on page 7, lines 26-27 with the following amended paragraph:

~~Figure 7 illustrates~~ Figures 7A-7D illustrate in flow diagram form the Data Exchange protocol by which a file transfer is made between sender and receiver.

4. Please replace the paragraph starting on page 10, line 36 to page 11, line 4 with the following amended paragraph:

Once the call has transferred to the recipient, the sender and recipient must exchange keys through a handshaking process. This is managed by the Key Exchange protocol, described in ~~Figure 5~~ Figures 5A-5C. Those ·skilled in the art will recognize that the steps in ~~Figure 5~~ Figures 5A-5C have been simplified somewhat for clarity, including the elimination of time outs and other internal testing for data integrity. Data flow between the sender and recipient is shown by a dashed line.

5. Please replace the paragraph on page 11, lines 5-13 with the following amended paragraph:

The protocol of ~~Figure 5~~ Figures 5A-5C begins at step 350 with the sender generating an appropriately secure key, for example a Diffie-Hellman random exponent eA and computing the related value $g^{eA}$ mod n, where g and n are fixed system-wide parameters. The sender also generates a 20-byte pseudorandom value, RandomA. Then, at step 355, the sender modem contacts the recipient modem. The recipient modem answers the modem call at step 360, which causes the sender to initiate a handshake session at step 365 by sending a first handshake packet, Handshake Packet A1. The first handshake packet sent by the sender includes the sender's version information, account number, $g^{eA}$ mod n, and a hash of RandomA. The data structure may be, for example:

6. Please replace the paragraph starting on page 12, line 31 to page 13, line 1 with the following amended paragraph:

The string X is then displayed as a pop-up window at the sender side, as shown in Figure 6A, and the sender is instructed to telephone the recipient to provide the string X. On the recipient side, shown in Figure 6B, the recipient is instructed to await a call from the sender and to insert the string X. These steps are shown in ~~Figure 5~~ Figures 5A-5C as steps 475 and 480, respectively. If the ID is confirmed, as checked at step 485 on the sender side and step 490 on the recipient side, the long term key LTK is saved at steps 495 and 500, respectively, followed by an exit. If the check at steps 485 and 490 results in a negative compare, the long term key is not saved and the process simply exits.

7. Please replace the paragraph on page 13, lines 6-9 with the following amended paragraph:

Once the Key Exchange protocol of ~~Figure 5~~ Figures 5A-5C is completed, the system moves on to the Data Exchange protocol shown in ~~Figure 7~~ Figures 7A-7D. As with ~~Figure 5~~ Figures 5A-5C, the flow diagram of ~~Figure 7~~ Figures 7A-7D is idealized and simplified, and data flow between the sender and recipient processes is shown with a dashed line.

8. Please replace the paragraph on page 13, lines 24-26 with the following amended paragraph:

Once the encryption is complete, the sender establishes a data connection with the recipient, as shown in ~~Figure 7~~ Figures 7A-7D at step 615. The sender then transmits to the recipient, at step 620. Transfer Packet A1 having a data structure as follows:

9. Please replace the paragraph on page 16, lines 29-34 with the following amended paragraph:

It can ~~therefor~~ therefore be appreciated that a new and novel system and method for secure communications of a wide variety of types of data has been described. It will be appreciated by those skilled in the art that, given the teachings herein, numerous alternatives and equivalents will be seen to exist which incorporate the invention disclosed hereby. As a result, the invention is not to be limited by the foregoing exemplary embodiments, but only by the following claims.